DEPARTMENT OF THE ARMY
HEADQUARTERS, 4th INFANTRY DIVISION
FORT HOOD, TEXAS 76544-5200

AFYB-CG

22 March 2007

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: 4ID, G6 Information Assurance (IA) Policy # 8: Intrusion Detection Systems

1. References:

a. AR-25-1, Army Knowledge Management and Information Technology, 15 July 2005.

b. AR 380-19, Information Systems Security, 27 February 1998.

c. AR 380-67, Personnel Security Program, 9 September 1988.

d. DoD Directive 8500.1, "Information Assurance (IA)", 24 October 2002.

e. DOD Instruction 8500.2, "Information Assurance (IA) Implementation", 6 February 2003.

f. DoD Instruction 5200.40, DoD Information Technology Security Certification and Accreditation (C&A) Process, 30 December 1997.

g. DoD CIO Guidance and Policy Memorandum (G& PM) No. 8-8001 - "Global Information Grid (GIG)," 31 March 2000.

h. DoD CIO Guidance and Policy Memorandum No 6-8510, "Department of Defense GIG Information Assurance and Information Assurance Implementation Guide", 16 June 2000.

2. Purpose of Policy:

a. Technical controls shall be adopted to ensure the reliability, availability, and integrity of these resources, while regulating access to systems that process sensitive but unclassified information.

b. Various network-monitoring tools exist to enable support employees to troubleshoot and correct problems. These tools exist in both hardware and software forms, and offer a wide range of options. Used correctly, these tools are invaluable for examining the network traffic at a detailed level. However, these tools can also be used to violate system and network integrity by examining packets to determine passwords and other access information. Other forms of misuse could include reading someone else's email and other restricted information.

3. Applicability: This policy applies to, and is an IT / IA operational directive to, all soldiers, civilians, and contractors who plan, deploy, configure, operate, or maintain data communications resources, IA systems, or firewall devices directly or indirectly attached to 4ID networks.

Responsibilities:

a. 4ID:

(1) Ensure that appropriate intrusion detection system (IDS) security policies are established.

(2) Prepare budget and funding requests to support the server and other Command and Control Protect (C2P) requirements.

b. Information Assurance Network Manager (IANM).

(1) Manage, audit, and respond to incidents identified by the 4ID IDS.

(2) Report incidents to the IAPM in a timely manner.

(3) Evaluate incidents to determine if security measures need to be modified to be more effective in preventing unauthorized access.

(4) In coordination with the IAM, appoint an Information Assurance Security Officer (IASO) and an assistant IASO with responsibility for reviewing IDS security logs.

(5) Ensure that the IDS system configuration is maintained current.

(6) Ensure that IA personnel are trained in the configuration and management of the intrusion detection technology.

c. Information Assurance Manager (IAM).

(1) Ensure that immutable server security logs are archived for central review by the designated IA staff.

(2) Ensure that servers are backed up on a scheduled basis. Verify monthly that the server backups can be restored.

d. Information Assurance Security Officer (IASO).

(1) Ensure intrusion detection systems are accredited in accordance with the DOD Directive 5200.40 and AR 25-2.

(2) Ensure intrusion detection systems are operated and maintained according to the vendor's specifications and organizational requirements.

(3) Working with the IANM, ensure intrusion detection system configuration and audit logs are reviewed frequently.

(4) Report any security incidents involving intrusion detection systems as required by the organizational security regulations, and to the IAPM.

(5) Ensure the intrusion detection systems security policy is implemented and carried out properly.

e. IDS System Administrator:

(1) Understand and monitor the configuration of the IDS technology.

(2) Make frequent backups of data and files on the IDS system and ensure that IDS software integrity is maintained.

(3) Respond to any alarms or alerts from the IDS software as quickly as possible.

(4) In coordination with the IASO, ensure adequate security is maintained over the IDS technology.

(5) Review IDS audit logs on a daily basis.

(6) Report any attacks or incidents on the IDS to the IASO.

(7) Evaluate each new release of the IDS software to determine if an upgrade is required and install all security patches directed by ACERT or recommended by the vendor.

4. Policy:

a. System and Security Logs:

(1) Systems Administrators shall enable auditing on all IDS hosts for hosts that provide this capability. The auditing shall encompass the appropriate security-related settings to include, but are not limited to: Logon/logoff accesses, object accesses, use of rights/permissions, security policy changes, and system restarts/shutdowns.

(2) Systems Administrators shall ensure that system audit/log files are saved off in a secured and adequately protected area and backed up on a regular basis. When possible, log files shall be saved off to networked servers for backup. These files shall be accessible by only the Systems Administrators and the IASO/IAM/IANM/IAPM.

(3) Systems Administrators shall ensure that system security logs are configured to not overwrite events, if the system so allows. The security logs shall be cleared manually so that no security-related events go without auditing. If there is an automated measure in place that prevents the over-writing of security logs until they are first backed up, it may be configured in lieu of the manual clearing of logs.

b. Intrusion Detection:

(1) In addition to intrusion detection system (IDS) monitored and managed by U.S. Army NETCOM at Ft. Huachuca, the 4ID IANM shall be authorized to place IDS technology in strategic locations on the network infrastructure to immediately detect the following:

(a) Attempts to gain unauthorized access to network and infrastructure resources,

(b) Denial of service attacks,

(c) Web site defacement, and

(d) Other actions that would compromise the integrity of the infrastructure or data processed thereon.

(2) Intrusion detection or network monitoring systems shall be configured and maintained to detect or intercept the latest hacking or other schemes of data mischief or destruction.

(3) When possible, the intrusion detection system or network monitoring system shall be configured with automated security measures that prevent further breaching from a specific exploitation source.

(4) Intrusion detection system logs from all 4ID managed intrusion detection systems shall be captured immediately and analyzed in accordance with procedures developed under the direction of the IAM and IANM.

(5) The IDS may be augmented with additional approved software to aid in the automated review of IDS logs and enhance the reporting and notification capability of the system.

c. Monitoring: Unless specifically authorized by the 4ID IAM, IANM, or IASO, no network monitoring equipment shall be used on the installation network outside of the 4ID, EOM. Monitoring will only be performed for network management/maintenance or in conjunction with an officially authorized investigation. Authorized 4ID Brigade Combat Teams and attached units may install and operate IDS on LANs that they operate, as long as they are operated in accordance with all governing laws and regulations.

5. Non-compliance: Improper use of monitoring equipment or software will be reported to the 4ID IAPM for action as deemed appropriate.

6. POC for this policy is the 4ID Information Assurance at DSN 737-0785 or commercial 254-287-0785.

JEFFERY W. HAMMOND
MG, USA
Commanding

DISTRIBUTION:
4ID
Organizations Attached to 4ID Networks